


Air Live[®]
www.ovislink.com.tw

Outdoor AP

WHP-1100, WHP-1120 & WHP-1130

User's Manual



Powered by OvisLink Corp.

TRADEMARKS

All names mentioned in this document are trademarks or registered trademarks of their respective owners.

The manufacturer provides this document “as is,” without warranty of any kind, neither expressed nor implied, including, but not limited to, warranty of fitness for the particular purpose for which it is intended. The manufacturer may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time. This document may include technical inaccuracies and/or typographical errors.

Packing List

Your Outdoor Access Point package should contain the following items:

- One Outdoor Access Point
- One DC injector with RJ-45 LAN and ODU (outdoor unit) jacks
- One power adapter for the DC injector
- One mounting kit
- One 25-meter Category 5 waterproof cable with RJ-45 plug and ODU connector
- One 30-cm Reverse N(M)-N(M) RG400 cable
- WLAN Management System software and outdoor access point user's guide in electronic form (one CD-ROM)

Contents

INTRODUCTION	1
RELATED PRODUCTS	2
WLAN MANAGEMENT SYSTEM	3
AUTOMATIC DISCOVERY OF COMPATIBLE DEVICES	3
WLAN MANAGEMENT SYSTEM HARDWARE AND SOFTWARE REQUIREMENTS	5
TERMINOLOGY USED IN THIS GUIDE	6
HOW TO USE THIS GUIDE	7
PLANNING THE NETWORK	8
INFRASTRUCTURE NETWORK TYPES	8
PLANNING AN INFRASTRUCTURE NETWORK	10
<i>Single AP Installation</i>	10
<i>Multiple AP Installation</i>	10
ROAMING	10
HARDWARE DESCRIPTION	12
HARDWARE PRE-CONFIGURATION	14
WIRELESS PRODUCT PLACEMENT GUIDELINES	15
INSTALLING THE WLAN MANAGEMENT SYSTEM	16
USING THE WLAN MANAGEMENT SYSTEM	19
AUTO-DISCOVERY	19
KICK START FUNCTION	20
CONFIGURATION	22
<i>Config Window – IP Panel</i>	22
<i>Config Window – Filter Panel</i>	23
<i>Config Window – Wireless Panel</i>	24
<i>Config Window – MAC Access Control Panel</i>	26
<i>Config Window – Encryption Panel</i>	27
<i>Config Window – SNMP Access Control Panel</i>	28
<i>Config Window – IEEE 802.1X Panel</i>	30
<i>Config Window – Trap Server Panel</i>	33
<i>Config Window – Advanced Panel</i>	35

MONITOR	35
<i>Identity Information</i>	36
<i>Statistics</i>	37
<i>Stations</i>	37
RESTART	38
FACTORY RESET	38
UPGRADE FIRMWARE.....	39
ADVANCED SETTINGS.....	40
BATCH MODE OPERATION	40
MANAGE WMS HOST TABLE	40
<i>Exporting a Configuration Profile to a File</i>	42
<i>Importing a Configuration Profile from a File</i>	42
FAQS	45
TROUBLESHOOTING	46
TECHNICAL SUPPORT	47
LIMITED WARRANTY	48
REGULATORY DOMAINS AND CHANNELS	51

FIGURES

FIGURE 1. SIMPLE WIRELESS INFRASTRUCTURE NETWORK.....	8
FIGURE 2. SINGLE-AP NETWORK.....	9
FIGURE 3. MULTIPLE-AP NETWORK.....	9
FIGURE 4-1. OUTDOOR ACCESS POINT AND DC INJECTOR.....	12
FIGURE 4-2. OUTDOOR ACCESS POINT INSTALLATION.....	13
FIGURE 5. MAIN MENU OF INSTALLATION CD-ROM.....	16
FIGURE 6. WELCOME WINDOW.....	17
FIGURE 7. CHOOSE DESTINATION LOCATION WINDOW.....	17
FIGURE 8. SELECT PROGRAM FOLDER WINDOW.....	18
FIGURE 9. SETUP COMPLETE WINDOW.....	18
FIGURE 10. WMS HOSTS VIEW WINDOWS.....	20
FIGURE 11. WLAN KICK START WINDOW.....	21
FIGURE 12. CONFIG WINDOW — IP PANEL.....	22
FIGURE 13. CONFIG WINDOW — FILTER PANEL.....	23
FIGURE 14. CONFIG WINDOW — WIRELESS PANEL.....	24
FIGURE 15. CONFIG WINDOW — MAC ACCESS CONTROL PANEL.....	26
FIGURE 16. CONFIG WINDOW — ENCRYPTION PANEL.....	27
FIGURE 17. CONFIG WINDOW — SNMP ACCESS CONTROL PANEL.....	29
FIGURE 18. NEW/EDIT ADDRESS DIALOG BOX.....	29
FIGURE 19. IEEE 802.1X PANEL — AUTHENTICATION OPTIONS.....	30
FIGURE 20. IEEE 802.1X PANEL — ACCOUNTING OPTIONS.....	31
FIGURE 21. IEEE 802.1X PANEL — RADIUS SETTINGS.....	32
FIGURE 22. CONFIG WINDOW — TRAP SERVER PANEL.....	33
FIGURE 23. TRAP SERVER PANEL — CLEAR ALL ADDRESS FUNCTION.....	34
FIGURE 24. TRAP VIEW WINDOW.....	34
FIGURE 25. WARNING BEFORE AP RESET.....	35
FIGURE 26. MONITOR COMMAND IN POP-UP MENU.....	36
FIGURE 27. MONITOR WINDOW — IDENTITY PANEL.....	36
FIGURE 28. MONITOR WINDOW — STATISTICS PANEL.....	37
FIGURE 29. MONITOR WINDOW — STATIONS PANEL.....	38
FIGURE 30. WARNING BEFORE AP RESTART.....	38
FIGURE 31. WARNING BEFORE FACTORY RESET.....	39
FIGURE 32. UPGRADE FIRMWARE DIALOG BOX.....	39
FIGURE 33. BATCH MODE OPERATION LIST.....	40
FIGURE 34. NEW/EDIT ADDRESS DIALOG BOX.....	41
FIGURE 35. EXPORTING A CONFIGURATION PROFILE TO A FILE.....	42
FIGURE 36. IMPORTING A CONFIGURATION PROFILE FROM A FILE (1).....	42
FIGURE 37. IMPORTING A CONFIGURATION PROFILE FROM A FILE (2).....	43
FIGURE 38. ENCRYPTION DIALOG DURING IMPORTING A CONFIGURATION PROFILE.....	43
FIGURE 39. IMPORTING A CONFIGURATION PROFILE FROM A FILE (3).....	44

Introduction

Congratulations on choosing an Outdoor Access Point. This guide gives comprehensive instructions on installing and using the Outdoor Access Point (AP), and also explains how to install and use the WLAN Management System (WMS) software.

Related Products

11-Mbps Wireless products provide an integrated solution to your wireless networking requirements.

- For indoor applications: Access points, wireless workgroup bridges, wireless Ethernet clients, and wireless adapters with various bus interfaces (PCMCIA, USB, and PCI).
- For outdoor applications: The Outdoor Bridge connects two independent Ethernet LANs via a radio link, making expensive outdoor cabling unnecessary. High-gain directional antennas provide the greatest possible transmission range for Outdoor Bridge and Outdoor Access Point.
- Management tools: Wireless products support the industry-standard Simple Network Management Protocol (SNMP) and the SNMP-based WLAN Management System (WMS), a powerful set of utilities for managing not only devices but whole networks and inter-networks.

WLAN Management System

WLAN Management System (WMS) is a powerful network management system that is fully compatible with the industry-standard Simple Network Management Protocol (SNMP). It features:

- Automatic discovery of all compatible devices that are configured within the same subnet
- Individual and batch-mode remote management of compatible devices, including Multi-Monitor, Batch-Upgrade, Batch-Reset, and Batch-Load Default functions. Batch-mode operation is ideal when deploying multiple compatible products.
- A friendly end-user interface with a consistent look and feel.

Automatic Discovery of Compatible Devices

A powerful auto-discovery algorithm is built into WMS. With a simple click on the Auto Discovery icon, all compatible devices within the subnet will be discovered. This discovery feature is based on the following techniques:

- **DHCP client and IP recovery:** The Outdoor AP has a built-in DHCP client, and will request an IP address from a DHCP server so that SNMP management can be carried out. Should there be a failure of the DHCP server, the Outdoor AP will auto-assign itself an IP address (see next) and then automatically negotiate for a new IP address when the server recovers.
- **Auto-IP:** When the Outdoor AP cannot get an IP address from a DHCP server, it will auto-assign itself an IP address of 169.254.x.x and a subnet mask of 255.255.0.0. A Windows-based system configured as a DHCP client will use the same algorithm to assign itself an IP address in the same subnet. *When the DHCP server comes back on line, users may need to renew their stations' IP settings as described below;* otherwise, Windows may continue to use the previous IP address instead of executing the auto-IP procedure.

Windows 95/98

- step 1.** Click **Start/Run**, type *wiipcfg*, and click **OK**. The *IP Configuration* dialog box will open.
- step 2.** Select the network adapter you use to connect to the Outdoor AP. Click **Release**.
- step 3.** Click **Renew** to retrieve new information (IP address, subnet mask, and default gateway address) from the DHCP server. Click **OK** to save the changes and exit the program.

Windows NT 4.0

- step 1.** Click **Start/Programs/Command Prompt**. Type *ipconfig /release* (with a space after *ipconfig*) and press **Enter**.
- step 2.** Type *ipconfig /renew* (with a space after *ipconfig*) and press **Enter** to retrieve new information (IP address, subnet mask, and default gateway address) from the DHCP server.
- step 3.** Type *exit* and press **Enter**.

Windows 2000/XP

- step 1.** Click **Start/Programs/Accessories/Command Prompt**. Type *ipconfig /release* (with a space after *ipconfig*) and press **Enter**.
- step 2.** Type *ipconfig /renew* (with a space after *ipconfig*) and press **Enter** to retrieve new information (IP address, subnet mask, and default gateway address) from the DHCP server.
- step 3.** Type *exit* and press **Enter**.

WLAN Management System Hardware and Software Requirements

System requirements for installing and operating the WLAN Management System are:

- An x86-based microcomputer running Microsoft Windows 95, 98, Me, NT 4.0, 2000, or XP
- Microsoft Internet Explorer 4.01 or later
- A connection to an Ethernet network

Particular versions of Windows have the following additional requirements:

1. On Windows 95, Microsoft DCOM95 must be installed. You can obtain DCOM95 from the following Microsoft Web page:
<http://www.microsoft.com/com/dcom/dcom95/download.asp>
DCOM95 can also be found on the Microsoft Visual Basic 5.0 CD-ROM (Enterprise, Professional, or Standard edition), in the directory \Pro\Tools\DCOM95.
2. On Windows 98 (with the exception of Windows 98SE, which already includes this component), Microsoft DCOM98 must be installed. You can use the following link to download it:
<http://www.microsoft.com/com/dcom/dcom98/download.asp>
3. On Windows NT 4.0, Service Pack 4 or later must be installed.

Terminology Used in this Guide

BSSID, MAC ID

The BSSID (Basic Service Set ID) is a factory-set ID unique to each wireless product. It is identical to the MAC ID (Media Access Control ID). It allows each wireless product to be identified on the wireless network.

ESSID

An Extended Service Set ID (often referred to as Service Set ID, or SSID) identifies the wireless LAN domain that an AP is in. A domain is generally composed of wireless APs you are most likely to communicate with. You can type an existing domain name or create a new one that contains up to 32 characters.

Regulatory Domain

11-Mbps wireless products use the license-free ISM (Industrial, Scientific, and Medical) band to communicate through radio waves. Different countries offer different radio frequencies to be used as the ISM band. There are four frequency bands defined by IEEE 802.11: Japan (2.471 to 2.497 GHz), USA, Extended Japan, Canada, and Europe (2.4 to 2.4835 GHz), Spain (2.445 to 2.475 GHz), and France (2.4465 to 2.4835 GHz). To use 11-Mbps wireless products in a country not listed above, check with your government's regulating body to find the correct frequency band to use. All wireless products are supplied preset to the country of sale's frequency band.

WEP

WEP stands for Wired Equivalent Privacy. It is an encryption scheme that provides secure wireless data communications. WEP uses a 40-bit or 128-bit key to encrypt data. In order to decode the data transmission, all wireless clients on the network must use identical keys.

How to Use this Guide

This user’s guide gives complete instructions for installation and use of the Outdoor Access Point (AP).

Wireless products are supplied with factory set default network settings. Use the WMS (WLAN Management System) tool to change the default settings before introducing a new Outdoor Access Point to an already-established wireless network.

The WMS program is a simple-to-use, yet extremely powerful, SNMP-based utility for online central configuration and network management from a remote station on the same subnet. A trap management program is also provided to monitor/diagnose the compatible products.

Read through the next section, “Planning the Network,” to learn how to get the best possible performance from your wireless network.

Step 1: Plan the wireless network	See “Planning the Network” for details.
Step 2: Pre-configure the AP before installing it on an existing Ethernet network	See “Hardware Pre-configuration” for details.
Step 3: Install the AP on the Ethernet network	See “Install WLNA Management System,” for details.
Step 4: Carry out on-line configuration and management of the AP via WMS	See “Using the WLAN Management System” for details.

Planning the Network

Infrastructure Network Types

An infrastructure network is formed by several wireless stations and one or more access points (APs), with the stations within radio range of the AP or APs. Figure 1 depicts a typical infrastructure network topology.

There are three infrastructure network setups that are commonly used. It is a good idea to understand the possible network setups and configuration requirements before planning your wireless network.

Type 1. The simplest wireless infrastructure network is composed of one access point (AP) and a few wireless stations communicating via radio waves (Figure 1). This setup enables mobile stations to communicate with each other. The main benefit of this type of network is to extend the range of the network. If an AP is placed between the stations, the radio transmission distance is effectively doubled since wireless computer #1 can talk to wireless computer #2 through the AP. The drawback of this configuration is that the effective bandwidth is halved since all communication is relayed by the AP.

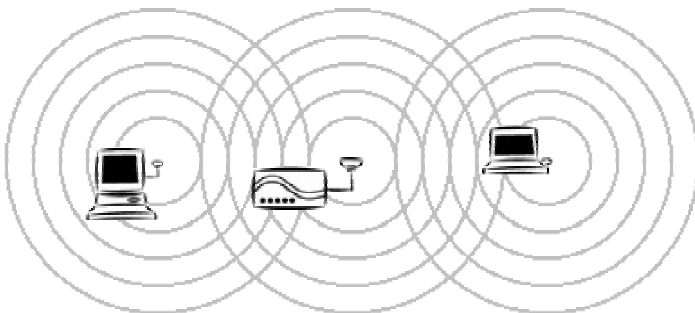


Figure 1. Simple wireless infrastructure network

Type 2. The next simplest wireless network is very similar to the Type 1 network. This time the AP is connected to a wired Ethernet network as a node. In this configuration the AP operates as a bridge between the wired Ethernet network and the wireless networks (Figure 2).

Wireless users have the same access to network resources as they would have if they were wired. Such a configuration is often used to allow roaming, or to extend an existing network into a hard-to-wire environment.

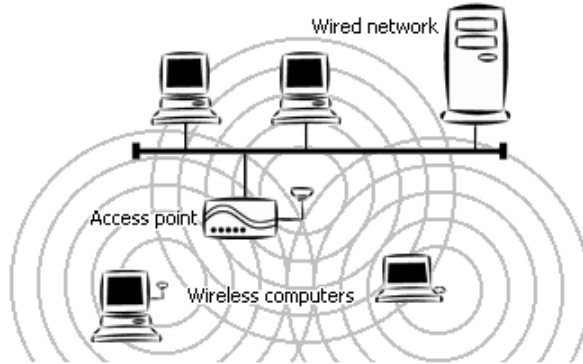


Figure 2. Single-AP network

Type 3. The third type of network is composed of multiple APs and multiple stations (Figure 3).

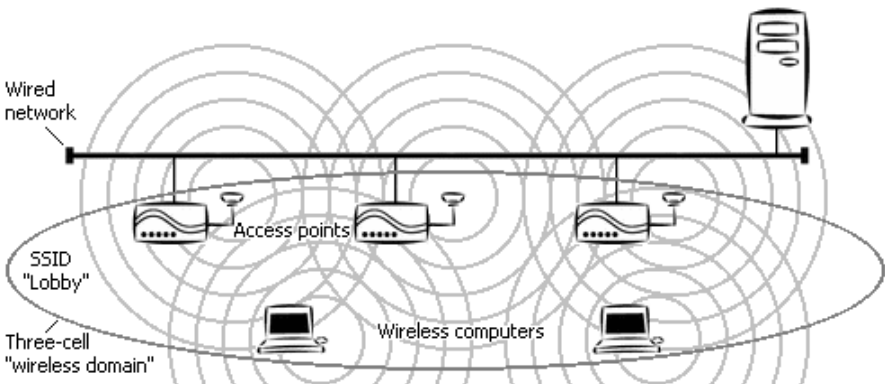


Figure 3. Multiple-AP network

The reasons for having multiple APs installed are:

1. To increase bandwidth in order to boost overall network performance
2. To extend the coverage range

Any other configuration is usually a mix of these commonly used types.

Planning an Infrastructure Network

This section explains some of the factors you need to consider when planning an infrastructure network. Setting up is a two-step process:

1. Install and configure the wireless products.
2. Decide the best physical location of the wireless products so as to optimize performance.

The following section gives quick guidelines for these two steps. First, decide whether to have a single AP wireless network or a multiple AP network.

Single AP Installation

If you are setting up a simple network with only one AP and a few stations (a Type 1 or Type 2 network configuration as described in “Infrastructure Network Types,” page 8), all you need to do is make sure the AP and all the wireless stations hold the same domain name (SSID) and security (WEP) settings in their configuration.

Adding a new station to an existing infrastructure network is easy. Again, all you need to do is to set the newly added station’s domain name (SSID) and security (WEP) settings to be the same as those of the AP.

Multiple AP Installation

Installing multiple APs on the same network (or domain) with overlapping signals (Figure 3)

- Use the same domain name (SSID) and security (WEP) settings.
- Enable the Roaming function on stations that require it.

Note: A station will automatically connect to whichever AP in the same domain is currently offering the best signal.

Roaming

Wireless products allow wireless stations to roam freely within an infrastructure domain composed of multiple APs with overlapping signal coverage (as in the Type 3 network configuration described in the previous section). For example, roaming

enables Station 1 to move from the AP 1 signal coverage area to the AP 2 signal coverage area without disconnecting from the network. The handover is achieved transparently; the Station 1 user would not realize he had moved from AP 1 to AP 2.

The requirements for a roaming environment are:

- a) Multiple APs with overlapping signal coverage (see “Multiple AP Installation.”)
- b) The APs must be configured to have the same domain name (SSID) and security (WEP) settings (see “Config Window – Encryption Panel.”).
- c) The mobile stations must have the same domain name (SSID) and security (WEP) settings as the APs.

It is advisable that APs on different TCP/IP subnets be given different domain names (SSIDs) to avoid roaming confusion (see the note below).

Note: For a mobile station to be able to move between APs without losing its network link, the Roaming function must be enabled on the station (this is automatic on some wireless LAN adapters), and the APs that the station roams to must be configured with the same domain name (SSID). If a station detects that the signal quality on the link to the current AP is poor, it will search for an AP in the same domain with better signal quality and automatically associate (establish a connection) with it. The station's IP address, however, will not change. A TCP/IP router will not route packets to a mobile station that has associated with an AP on a different TCP/IP subnet. In other words, if your network consists of two subnets connected by a router, a mobile station may roam to a different subnet with the same domain name (SSID) and then be unable to communicate with other network devices via TCP/IP. To avoid this problem, you should assign different domain names (SSIDs) to different TCP/IP subnets.

Hardware Description

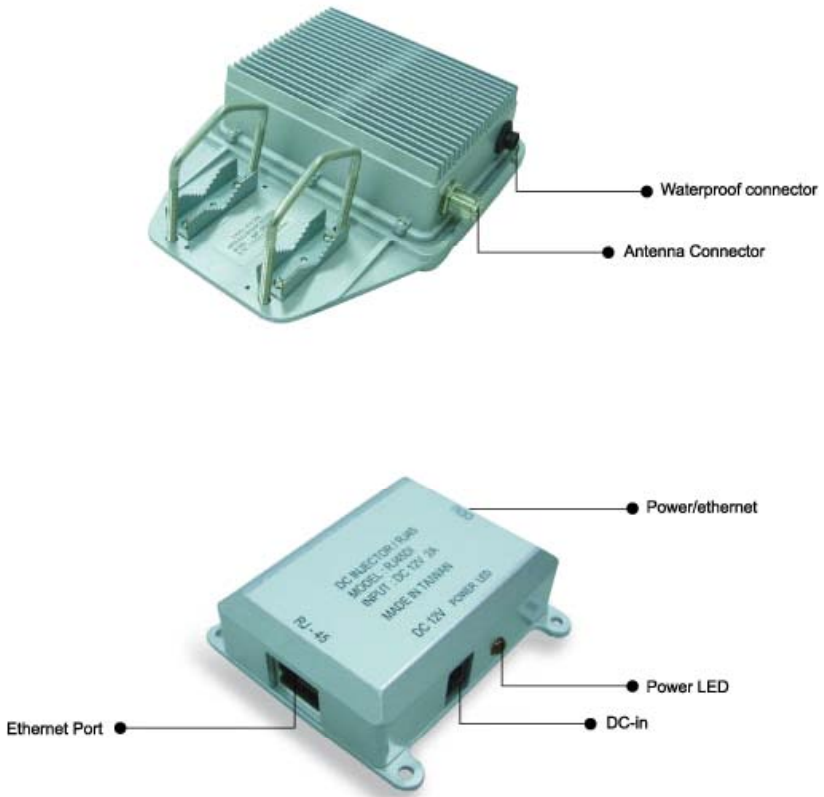


Figure 4-1. Outdoor Access Point and DC Injector

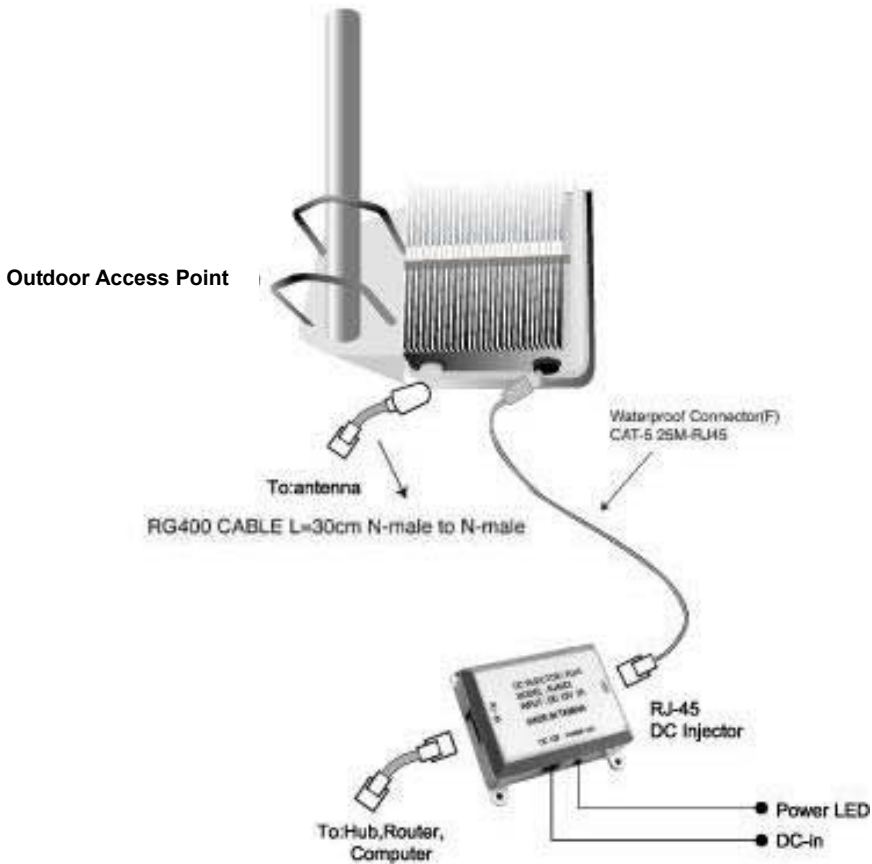


Figure 4-2. Outdoor Access Point Installation

Hardware Pre-configuration

Before adding the Outdoor Access Point to an existing Ethernet network, you may need to set basic parameters — SSID, security (WEP, and possibly 802.1x), AP name, channel number, and IP address — to make the AP compatible with the existing network.

Pre-configuration can also be carried out through WMS. As long as the AP and the management station are on the same physical Ethernet LAN, WMS's **Kick Start** function will find the AP and let you set basic parameters. Make connections as follows:

- step 1.** Using CAT5 waterproof cable, connect the waterproof connector port of the Outdoor AP to the ODU port of DC Injector.
- step 2.** Using Category 3 or higher UTP or STP cable, connect the RJ-45 port of DC Injector to a 10- or 10/100-Mbps Ethernet hub or switch, and connect the management station to a hub or switch on the same LAN.
- step 3.** Connect the output code of power adapter to the DC Injector's DC input jack, and plug it into an AC outlet to power up the Outdoor AP.

If a DHCP server is present, you can also connect the AP to the network, let it obtain IP settings via DHCP, and use WMS's **Auto Discovery** feature to learn (and optionally adjust) those settings.

Wireless Product Placement Guidelines

A few tips to mention that are particularly significant in a radio wave communications system:

1. Radio waves reflect or refract from buildings, walls, metal furniture, or other objects. This could result in performance degradation due to the fluctuation of the received signal.
2. Microwave ovens use the 2.45 GHz frequency band. 11-Mbps wireless devices also functions in the 2.4 ~ 2.5 GHz band, and therefore shares some of the band with microwave ovens. This means that when a nearby microwave oven is in use, it may interfere with 11-Mbps wireless signals, resulting in performance degradation on the wireless network.

Installing the Management Software

- step 1.** Insert the Installation CD-ROM in the CD-ROM drive and wait a few seconds while the drive spins up. A window such as that shown below will appear automatically.

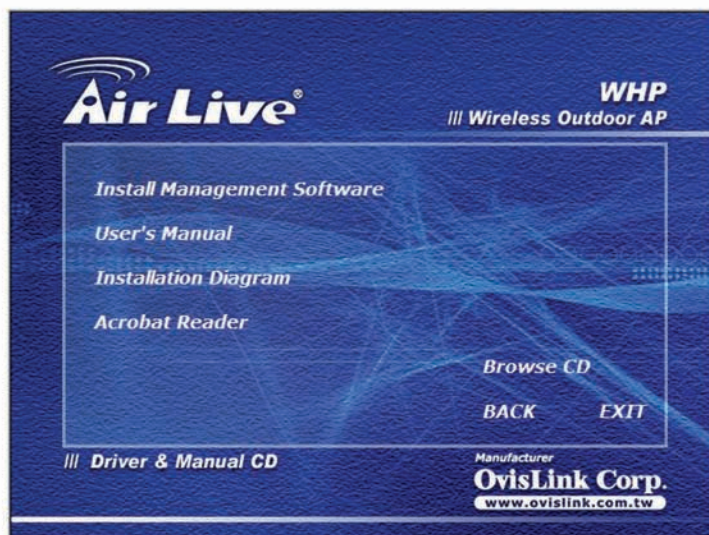


Figure 5. Main menu of Installation CD-ROM

- step 2.** Click *Install Management Software*. A *Welcome* window will then appear. Click *Next*.



Figure 6. Welcome window

- step 3.** Older operating systems may need to update some system files to function correctly with the WLAN Management System. If required, follow the on-screen instructions to download the required file. Click *Next* to open the *Choose Destination Location* window.

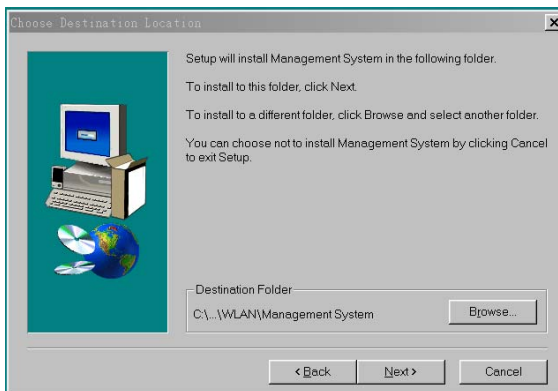


Figure 7. Choose Destination Location window

step 4. Click *Next*.

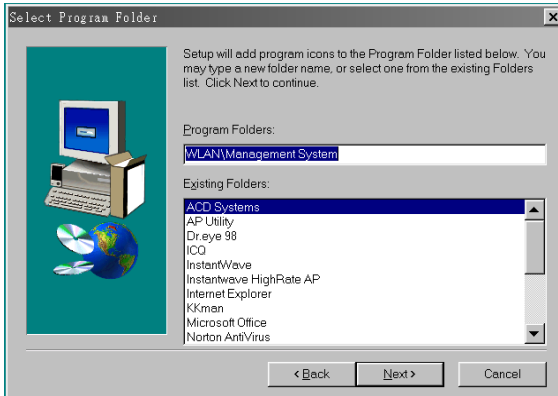


Figure 8. Select Program Folder window

step 5. Follow all on-screen instructions until the *Setup Complete* window appears.



Figure 9. Setup Complete window

step 6. Check “I would like to launch Management System” (Figure 9) and click *Finish*.

Using the WLAN Management System

Once the Outdoor AP is connected to an Ethernet network, a network administrator can connect to it from any PC on the same network via the WLAN Management System (WMS) utility.

The WMS utility is a Windows-based SNMP management tool allowing network administrators to remotely configure and monitor the Outdoor AP through both an Ethernet and a wireless connection. To launch the WMS utility:

step 1. Click *Start > Programs > WLAN > Management System > WLAN Management System*. The main WMS window will open. Click *Start/Start Hosts View*.

Auto-Discovery

This discovery protocol can discover all compatible wireless operating devices connected to the Ethernet LAN within the same subnet.

- step 1.** Click the Auto Discovery icon (a pair of binoculars) on the left side of the Hosts View window. All working compatible devices will automatically be discovered.
- step 2.** Select one of the wireless devices on the list. The utility buttons on the left toolbar will be enabled.
- step 3.** Right-clicking on a particular device will open a popup menu offering the same functions as the toolbar (Figure 10).

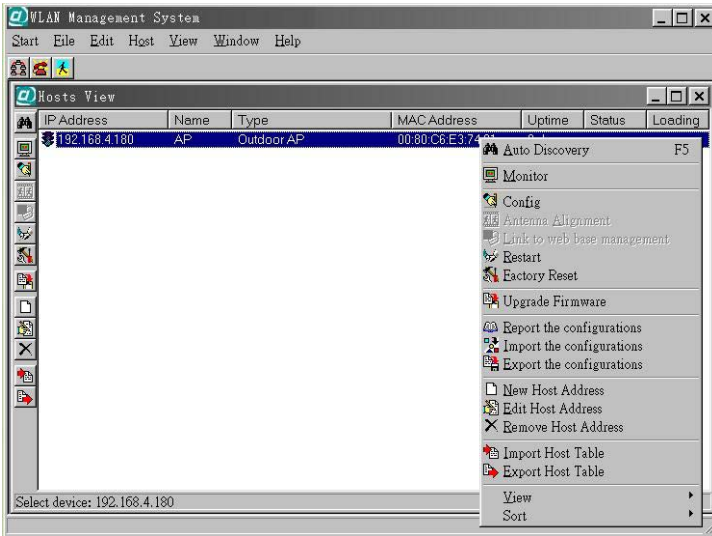


Figure 10. WMS Hosts View windows

Kick Start Function

If for any reason the AP does not yet have a reachable IP address, it can be discovered, and a suitable IP address assigned to it, using the Kick Start function.

- step 1.** Click the Kick Start icon (a figure with one leg extended) in the top toolbar. The *WLAN Kick Start* window will appear.
- step 2.** Open the *WLAN Kick Start* window's **Start** menu and choose *Find*, or click the Find icon (a pair of binoculars), or press F5. After a few seconds the MAC addresses of all Kick Start-compatible devices on the network will appear.
- step 3.** Select the device to be configured, open the **Tools** menu and choose *Change IP Settings* (or click the Change IP Settings icon).

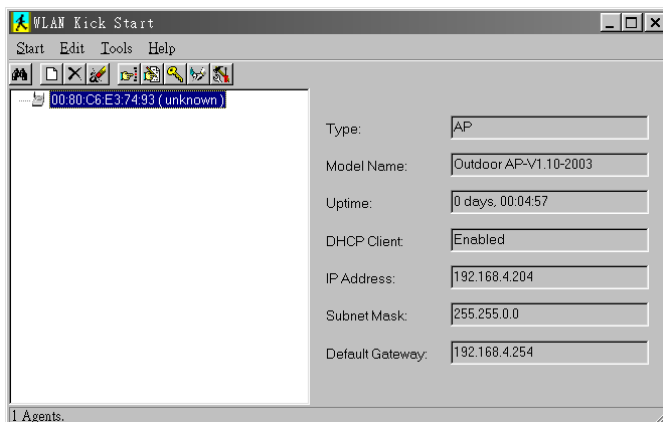


Figure 11. WLAN Kick Start window

This window's *Tools* menu also lets you test IP connectivity, reboot, reset the selected device, or change its password. The administrator password set on the device is "admin" as the default. The *Edit* menu is for manually adding and removing devices in the display. The *Start* menu, in addition to letting you initiate Kick Start discovery, lets you set preferences for the Kick Start and ping functions (timeout periods, number of tries, etc.).

Configuration

- step 1.** For configuration, select the Outdoor AP on the *Hosts View* window.
- step 2.** Right-click the Outdoor AP to open the popup menu (Figure 10).
- step 3.** Click **Config** to go to the configuration window (Figure 12).

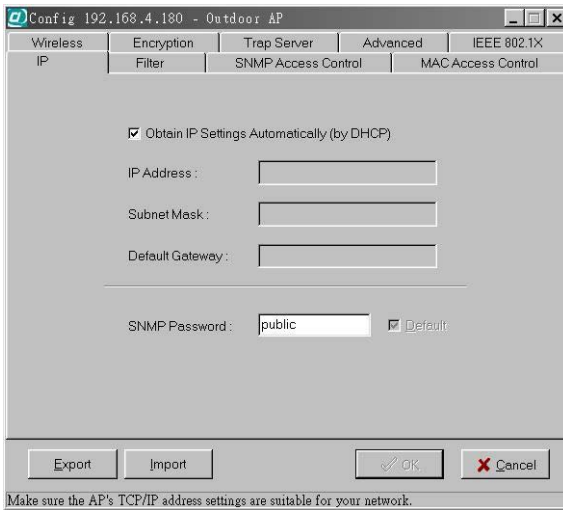


Figure 12. Config window — IP panel

Config Window – IP Panel

IP Address Setting: The Outdoor AP is a DHCP client. It will automatically ask the DHCP server to assign it an IP address. An administrator can assign a fixed IP to an Outdoor AP by unchecking the *Obtain IP Settings Automatically (by DHCP)* box (Figure 12). You may also configure a subnet mask and add a default gateway.

If you assign a fixed IP address to an Outdoor AP, make sure that all Outdoor APs within the same network have the same TCP/IP subnet address.

Obtain IP Settings Automatically (by DHCP)	Automatically retrieves an IP address for the Outdoor AP from a Dynamic Host Configuration Protocol (DHCP) server. This option is enabled by default.
IP Address	Manually assigns an IP address to the Outdoor AP.

Subnet Mask	Manually assigns a subnet mask to the Outdoor AP.
Default Gateway	Manually specifies the default gateway IP address (if required).

Note: An Outdoor AP will directly transfer SNMP response packets (confirmation packets) to a WMS PC if it is within the same LAN (the same subnet mask). If an SNMP response packet from an Outdoor AP is destined for a WMS PC on another LAN, the SNMP response packet needs to be forwarded by routers. The default gateway is the closest router to the Outdoor AP. If the correct default gateway is set, you can use a WMS manager (i.e. a PC running WMS) physically located in a different subnet to manage this Outdoor AP.

Config Window – Filter Panel

The next panel in the configuration dialog box is *Filter* (Figure 13).

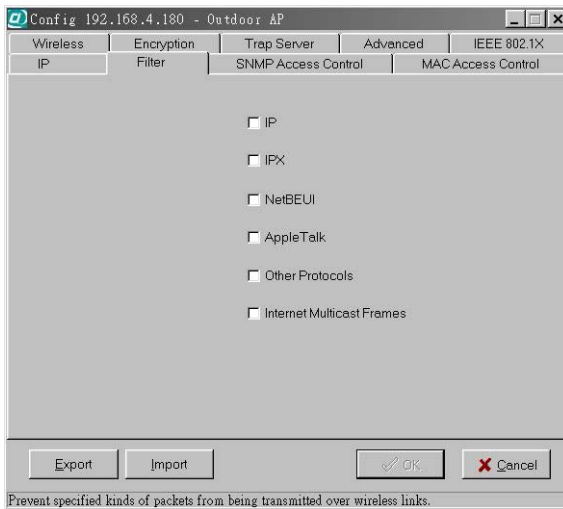


Figure 13. Config window — Filter panel

This is a one-way protocol filtering mechanism that prevents the Outdoor AP from transmitting specified protocols packet from a wired Ethernet LAN into the wireless LAN. If you do not require particular protocols on the wireless part of your network, you can save bandwidth by enabling the protocol filter.

From the **Filter** panel, some, all, or none of the protocols listed may be selected for filtering out:

- IP Protocol
- IPX Protocol
- NetBEUI Protocol
- AppleTalk Protocol
- Other Protocols
- Internet Multicast Frames

Config Window – Wireless Panel

The *Wireless* panel (Figure 14) provides access to the Wireless settings.

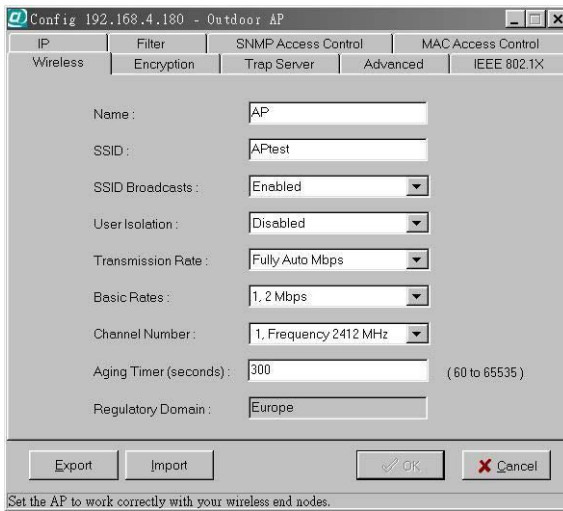


Figure 14. Config window — Wireless panel

These settings are explained in the following table.

Name	Assigns the Outdoor AP a unique name that allows the AP to be easily identified on the network.
SSID	Identifies the wireless LAN domain that this AP is in. A domain is generally composed of wireless APs you are most likely to communicate with. You can type an

	existing domain name or create a new one that contains up to 32 characters.
SSID Broadcasts	Click to enable or disable the SSID Broadcasts feature: If disabled, the Outdoor AP will: <ul style="list-style-type: none"> • Blocks a connection request from a station without the correct SSID. • Hides the SSID in outgoing beacon frames. A site-survey tool will not find the SSID.
Transmission Rate	Sets the transmission rate at which data packets are transmitted by the Outdoor AP. In high-interference environments a lower rate can increase overall transmission speed by reducing resends of lost packets.
Basic Rates	This value determines the basic rates used and reported for this BSS by the Outdoor AP. The highest rate specified is the rate that the Outdoor AP will use when transmitting broadcast/multicast and management frames. Available options are: <ul style="list-style-type: none"> • 1 and 2 Mbps • All (1, 2, 5.5, and 11 Mbps)
Channel Number	You can change the channel number from here. Refer to “Regulatory Domains and Channels” on page 51 for channels supported in each regulatory domain. If the “Automatically” option is selected, the access point can choose an available radio channel automatically.
Aging Timer (seconds)	The expiration time for WLAN station without activity.
Regulatory Domain	Identifies the country where the Outdoor AP is used. Each country has defined its available channel numbers and transmission power (see “Regulatory Domains and Channels”).

Important:

In a multiple cell network topology, overlapping and/or adjacent cells using different channels can operate simultaneously without interference if the difference between the center frequencies is at least 30 MHz. For example, channels 1, 7, and 13 are non-overlapping frequency channels.

Config Window – MAC Access Control Panel

This feature lets you limit access to the network through the access point. You can list up to 1000 stations that are to be granted or denied access. A drop-down box lets you select the method of access control:

- **Disabled:** Disable MAC-address access control. This is the default setting.
- **Accepted List:** Only wireless stations whose MAC addresses are on the list are allowed to connect through the access point.
- **Denied List:** Wireless stations whose MAC addresses are on the list are prevented from connecting through the access point.

To add a wireless station to the list, click the *New MAC Address* icon (a sheet of paper with one corner folded) on the left side of the MAC Access Control panel. You will be prompted to enter:

- The wireless station's MAC address.
- A name for the station.

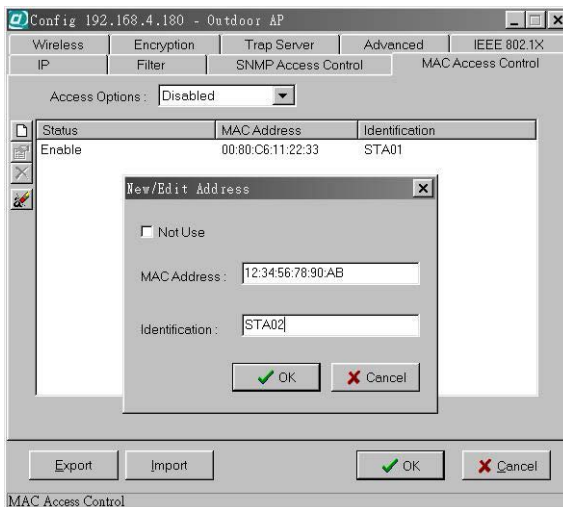


Figure 15. Config window — Mac Access Control panel

Wireless stations registered in the MAC Address Control Table can be individually turned on or off. For example, if you have enabled the Accepted List option, you can check the *Not Use* box for any listed station; the status of this station's entry will be

disabled, and the access point will then refuse all connection attempts from that station. Clear the *Not Use* box to let the selected method of access control take effect on this station.

MAC Address List:

Status	Disables or enables an individual entry
Address	The MAC address of a wireless station
Identification	Identification for the wireless station

Config Window – Encryption Panel

Click the *Encryption* tab (Figure 16) to set up the security options.

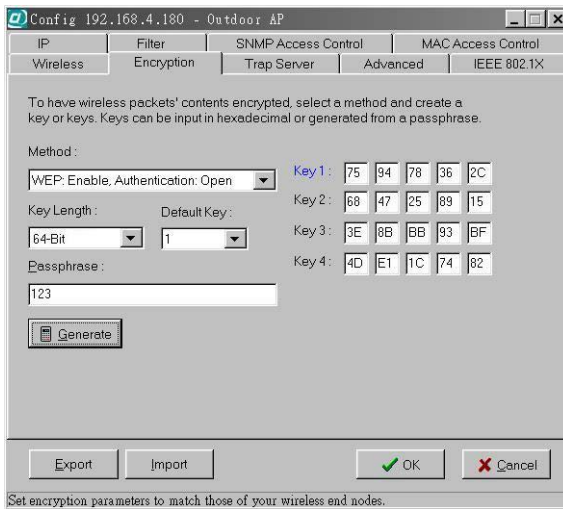


Figure 16. Config window — Encryption panel

The default setting is WEP disabled and initially the key sections are blank.

The pull-down *Method* box lists four options:

- **WEP: Disable, Authentication: Open** – Disable data encryption
- **WEP: Enable, Authentication: Open** – Enable data encryption and use Open System authentication (wireless clients’ requests to join the network *must not* be

WEP-encrypted)

- **WEP: Enable, Authentication: Shared** – Enable data encryption and use Shared Key authentication (such requests *must* be WEP-encrypted)
- **WEP: Enable, Authentication: Both** – Enable data encryption and use both Open System and Shared Key authentication (all requests are processed)

If enabled data encryption, there are two options in the pull-down *Key Length* box:

- 64-Bit - Enable use of 64-bit WEP
- 128-Bit - Enable use of 128-bit WEP

Key Generation - There are two ways to generate a security key. The first is by entering any text in the *Passphrase* field. Click the **Generate** button. For 64-bit WEP, it will generate four keys, Key 1, Key 2, Key 3, and Key 4. Select a key number from the dropdown list of the *Default Key* box. If you do not manually select a key, key 1 will be selected. For 128-bit WEP, only one key will be generated. Click **OK**.

Another WEP key generation method is to insert the key values directly from the keyboard. Enter your own key into one of the *Key 1~4* fields. Select that field number in the *Default Key* field.

Config Window – SNMP Access Control Panel

The AP contains an SNMP access table to limit access to its configurations. By default there is no restriction on accessing the AP. To avoid chaos on the network, access to the Outdoor AP configuration should be restricted to only those who require access.

When you select *SNMP Access Control*, the system will display four blank wireless devices for setting (maximum of 4 SNMP devices can be set). Right-click on a blank in the list and click **Edit Address** (Figure 17).

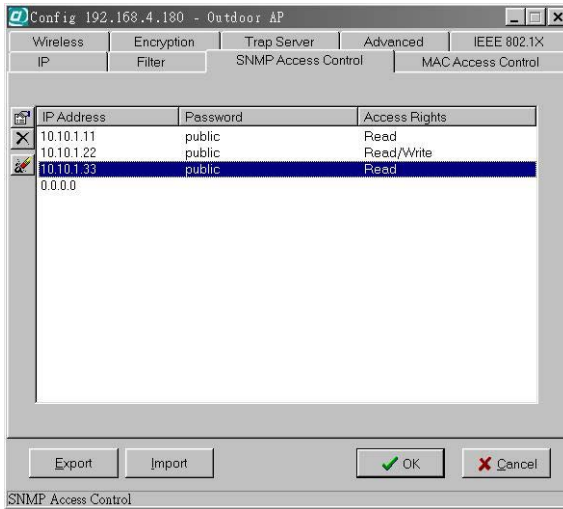


Figure 17. Config window — SNMP Access Control panel

The *New/Edit Address* dialog box will open (Figure 18).

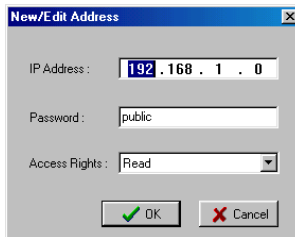


Figure 18. New/Edit Address dialog box

Two levels of access rights may be assigned:

Read	Read-only rights. The user may read everything except the Access Control settings, but is not allowed to alter anything
Read/Write	The user may read and alter all settings

Note: Do not set all the stations in the Access Control table to Read only. Once this is set and enabled, it will be impossible to modify the Outdoor AP. If this situation occurs, you need to reset the Outdoor AP to the factory configuration using Kick Start. (See FAQs for details)

To set a stations access rights, enter a station’s IP address and password and choose *Read* or *Read/Write*.

When a setting is made, click **OK**. Repeat the procedure for the next stations. When all settings are made, click **OK** in the configuration dialog box to make the changes effective.

Config Window – IEEE 802.1X Panel

The *IEEE 802.1X* panel allows you to set up 802.1x authentication on an Outdoor Access Point. Check *Enable 802.1X Access Control* box will activate the three subcategories of IEEE 802.1x related controls: Authentication Options, Accounting Options, and RADIUS Settings. These controls are illustrated and explained below.

Authentication Options

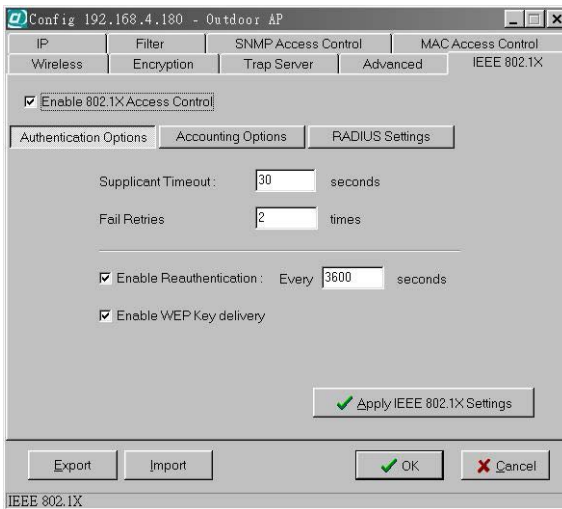


Figure 19. IEEE 802.1X panel – Authentication Options

Supplicant Timeout – This control sets the maximum time that the AP will wait for an authentication response from a client. Once this limit has been reached, the AP will check how many times it has tried (see next).

Fail Retries – This is the number of times the AP will restart the authentication process with the client before returning an error.

Enable Reauthentication – If this control is checked, the AP will re-initiate authentication whenever the specified amount of time has passed.

Enable WEP Key Delivery – If this control is checked, the AP will pass the WEP key to the client after the authentication procedure has finished. This only applies when the AP has WEP enabled, EAP-TLS is being used on the RADIUS server as the authentication method, and the supplicant has been authenticated with the RADIUS server.

Accounting Options

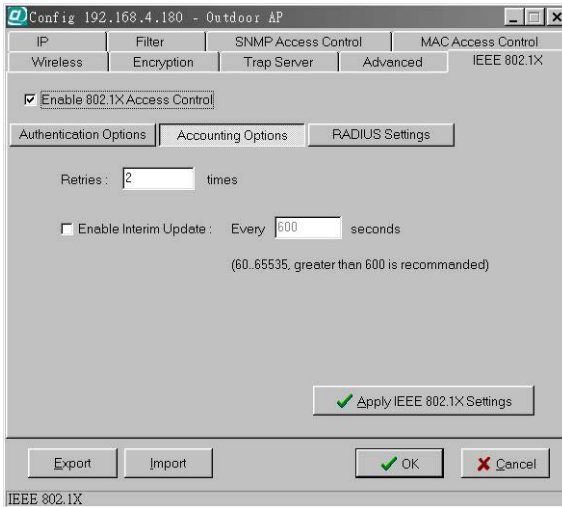


Figure 20. IEEE 802.1X panel – Accounting Options

Retries – This is the number of times the AP will attempt to resend accounting information to the server before returning an error.

Enable Interim Update – If this control is checked, the AP will periodically resend any accounting information to the server. The update time can be set by the user.

RADIUS Settings

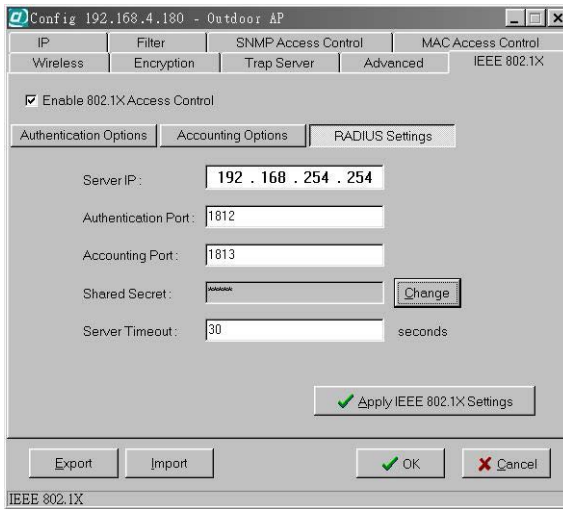


Figure 21. IEEE 802.1X panel – RADIUS Settings

Server IP – This is the RADIUS server’s IP address. This must be set in order for the AP to communicate with the server.

Authentication Port, Accounting Port – These are the port numbers that the server is using to listen for incoming accounting and authenticating packets. These can be set manually on the server but must be set here as well. These are advanced options and the defaults will work without further configuration.

Shared Secret – The shared secret is set on the server as part of the 802.1x protocol. It is a key used for encryption between the authenticator and the server. The key set here must be the same as the one set on the server, or the AP and the server will not be able to communicate.

Server Timeout – This is the maximum time that the AP will wait for the RADIUS server to respond. If there is no response within this time, the AP will return an error.

Click **Apply IEEE 802.1X Settings** button to turn on 802.1x support on the AP immediately without reset. Once this is done, normal traffic will not be forwarded without authentication.

Config Window – Trap Server Panel

When the Outdoor AP is powered on, or an Ethernet port becomes active, an event log will be generated indicating the time, the IP address of the reporting Outdoor AP, and the event. You can view and save the event logs from the station as a Trap Server.

To assign a trap server, click Trap Server (Figure 22).

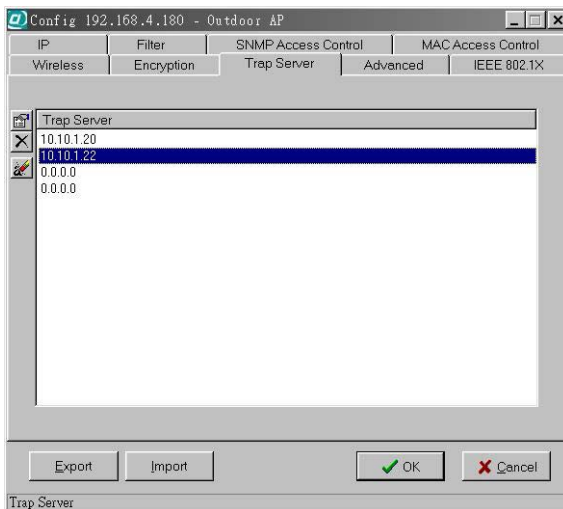


Figure 22. Config window — Trap Server panel

Assign a station as a trap server by entering its IP address. Right-click on a blank in the list and click **Edit address**.

To remove a trap server from the list, highlight it and click **Clear address**. Click **Clear all address** to remove all assigned trap servers from the list (Figure 23).

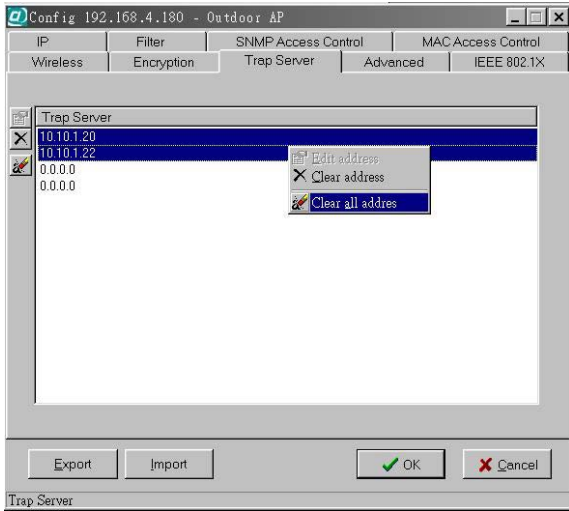


Figure 23. Trap Server panel — Clear all address function

Trap View

To view trap log information, click the *Start Trap View* icon (a ringing telephone) in the upper left corner of the main WMS window. A window such as that shown below will appear (Figure 24).

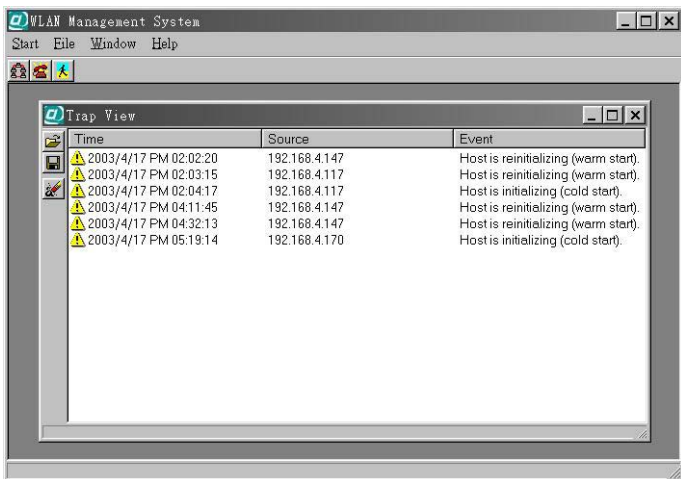


Figure 24. Trap View window

The log shows the time, the IP address of the reporting Outdoor AP, and the event. You can save, open, and delete log files through the *File* menu.

Config Window – Advanced Panel

You may set the packet size of RES Thresholds and Fragmentation Thresholds in the *Advanced* panel. The panel also contains a ***Tx Power (mW)*** control with options for setting the AP’s transmitter power to 5, 10, 30, 50, or 100 mW.

Important:

Once all configurations have been completed, click ***OK***. You will be reminded that a reset is required to make the changes effective. Click ***Yes***.

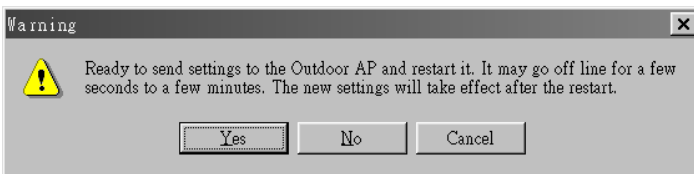


Figure 25. Warning before AP reset

Monitor

The Monitor tool allows the Outdoor AP’s status, Ethernet statistics, wireless statistics, and other configuration information to be viewed/monitored.

In the *Hosts View* window (Figure 26), select a device and click the ***Monitor*** button on the toolbar or on the popup menu.

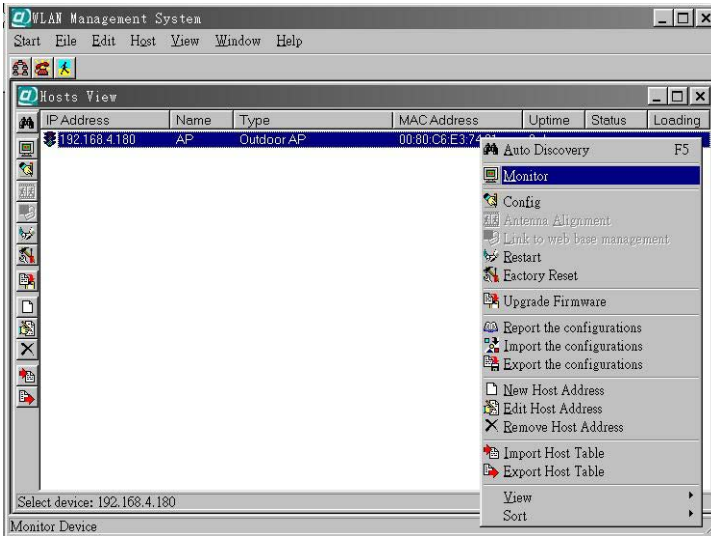


Figure 26. Monitor command in pop-up menu

An *information* window will appear. The first of three panels in this window, the Identity panel, will be visible (Figure 27).

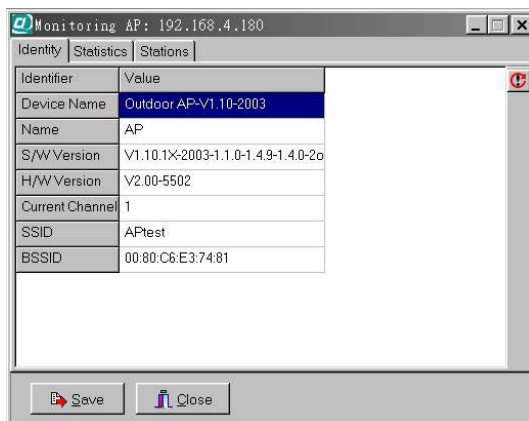


Figure 27. Monitor window — Identity panel

Identity Information

The information shown (see table below) is read-only.

Device Name	WMS system default category name
-------------	----------------------------------

Name	Human-friendly name assigned by the user for easier identification
S/W Version	Shows the device software version number
H/W Version	Shows the device hardware version number
Current Channel	Shows the wireless channel currently in use on the device
SSID	Shows the SSID of the device
Current BSSID	Shows the BSSID of the device (same as the device MAC address)

Statistics

The *Statistics* window shows both Ethernet and wireless transmission/reception statistics. To refresh the statistics, click on the ► button to continually refresh the information. Click on the ■ button to stop updating the information.

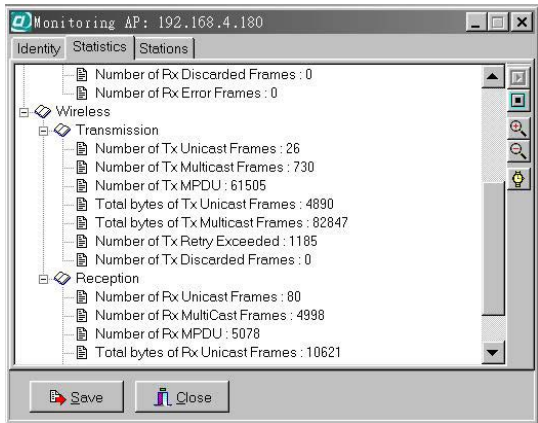


Figure 28. Monitor window — Statistics panel

Stations

The *Stations* window lists all the currently associated wireless station’s Media Access Control (MAC) addresses.

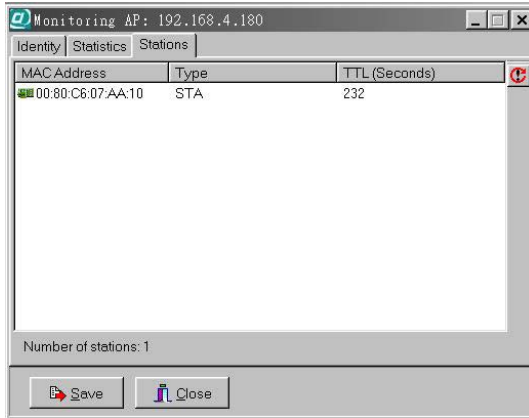


Figure 29. Monitor window — Stations panel

Restart

Restarting the Outdoor AP will take about 30 seconds (Figure 30).

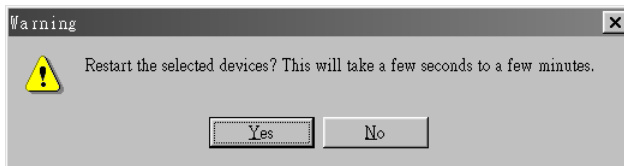


Figure 30. Warning before AP restart

During this period, the WMS program will not be able to query the Outdoor AP via the SNMP protocol and the Outdoor AP will not be available to its client stations. If you try to access the device, the WMS program will display the message “Timeout! No response from agent.”

Factory Reset

Click *Factory Reset* if you want to return the Outdoor AP to its factory default settings. A warning dialog box will open (Figure 31).

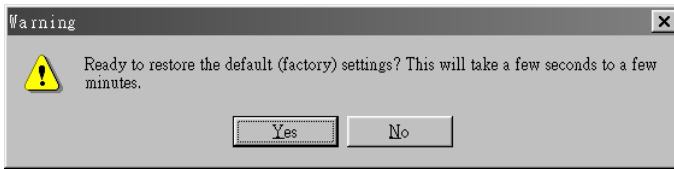


Figure 31. Warning before Factory Reset

Click **Yes** to return the Outdoor AP to the factory default settings.

Upgrade Firmware

The Outdoor AP's embedded software is contained in "flash" ROM, and can be updated over your LAN via the WMS program. To download new embedded software to the device, click *Upgrade Firmware*. The *Upgrade Firmware* dialog box will open (Figure 32).

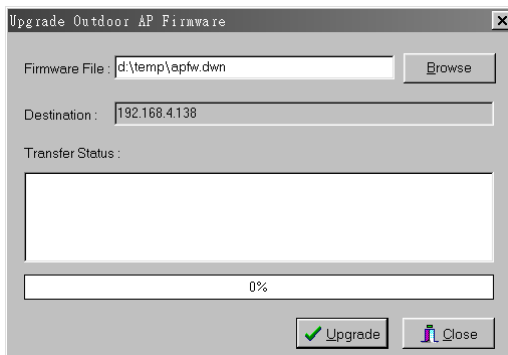


Figure 32. Upgrade Firmware dialog box

Browse for the file to be uploaded to the Outdoor AP, or type the path and file name into the *Firmware File* field.

The *Upgrade* button will then become enabled. Click **Upgrade** to start downloading the file to the Outdoor AP. The WMS and the Outdoor AP's built-in Trivial File Transfer Protocol (TFTP) client/server will load the new executable into the Outdoor AP's flash ROM area. If the download activity fails, an error message will be shown in the message box. Once the file transfer is complete, click **Close** to close the window.

Advanced Settings

Batch mode operation

In order to maximize the efficiency of wireless LAN management, you can use batch mode operation to manage selected APs or other wireless devices. You can sort wireless devices by device type first. Then select the multiple APs or other devices you would like to manage. Next, click the right mouse button to open the tool bar; then choose the functional tool you would like to use to work on these specific APs or other devices.

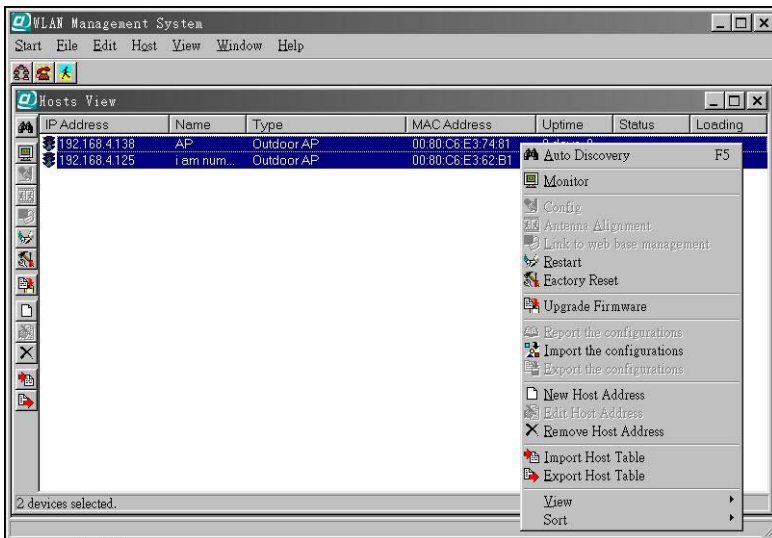


Figure 33. Batch mode operation list

Manage WMS Host Table

Partition the network according to the physical location

The Host Table is a very powerful function to support a mass deployment of wireless products. You can combine several Outdoor Access Points together with Outdoor Bridges or other wireless devices to form a group with a specific Host Table name so that you can divide the wireless network into many small groups.

Create Host Table via Automatic Discovery

Click *Automatic Discovery* icon to find all compatible devices. Select the desired APs and other wireless devices (for example, located in building A). Click the right mouse button to open the popup menu. Choose ***Export Host Table*** to save the Host Table to a file (for convenience, you can save the Host table on a network disk for ease of access).

Import Host Table to check device's availability

Import the Host Table from a file (for convenience, you can retrieve the Host table on a network disk for the ease of access). Once the Host Table is imported, WMS will automatically check the availability of APs and other compatible devices listed in the Host Table. This is an extremely powerful feature to make up for the inadequacy of Auto-Discovery. Auto-Discovery can only find compatible devices when they are alive. Failed devices cannot be found via Auto-Discovery. The devices listed in the Host Table should be available and provide the service. If they do not exist, WMS can report their absence immediately so that the system administrator can take immediate action.

New/Edit/Delete a Host Address on Host Table

Click the *New Host Address* button to open the New/Edit Address dialog box (Figure 34). After enter the Outdoor AP's IP address, WMS will automatically find the device and list it on the Host Table. You can also select any Outdoor AP on the table and click the *Remove Host Address* button to delete it whenever it is no longer necessary.

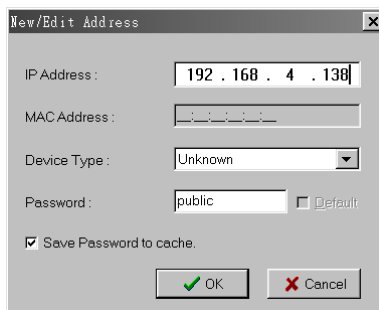


Figure 34. New/Edit Address dialog box

Exporting a Configuration Profile to a File

The configuration file can be saved to a text file and safely kept. This configuration file can also be imported to recover the wireless Product's setting, if there is an accident. This profile can also be copied to the other wireless product of the same kind. To do this, first click the *Export* button in the *Configuration* window. Then enter the file name for the configuration profile to be saved to.

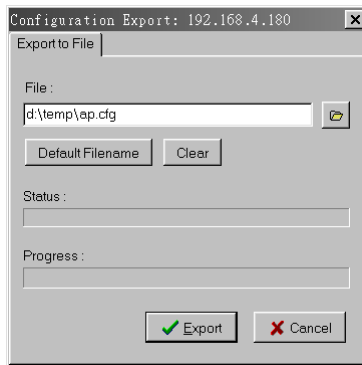


Figure 35. Exporting a configuration profile to a file

Importing a Configuration Profile from a File

A configuration file can also be imported to recover the Outdoor AP's original settings. This profile can also be copied to the other Outdoor APs. To do this, first click the *Import* button in the *Configuration* window. Then enter the file name for the configuration profile to be imported from. Click *Next*.

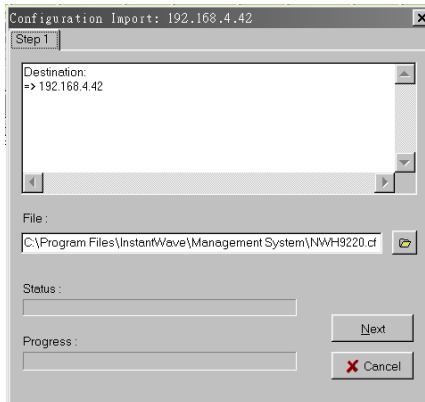


Figure 36. Importing a configuration profile from a file (1)

On Step 2 screen, you can select or clear the sessions of the configuration profile to be imported. Click *Next*.

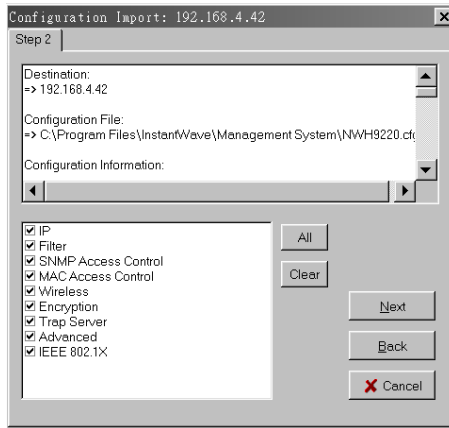


Figure 37. Importing a configuration profile from a file (2)

Encryption

The configuration profile does not contain the security key settings. The attributes of security keys are externally **write-only** and cannot be saved into the configuration file. If you select Encryption session to be imported, it will display the *Encryption* window before Step 3 screen and ask you to enter the security key settings manually.

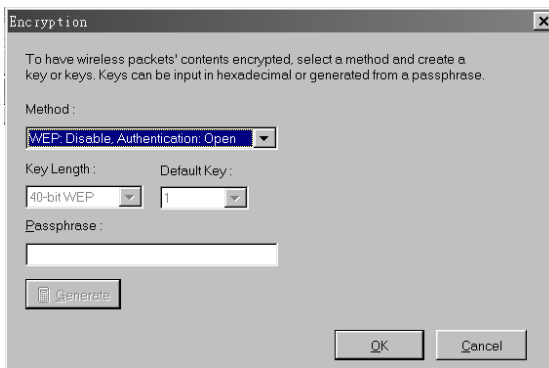


Figure 38. Encryption dialog during importing a configuration profile

On Step 3 screen, click *Import*.

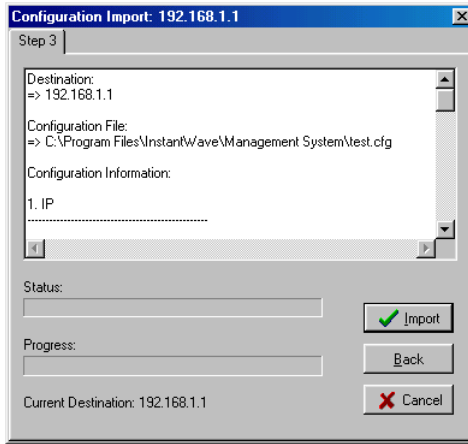


Figure 39. Importing a configuration profile from a file (3)

FAQs

The FAQs section attempts to answer the most commonly asked questions about Outdoor Access Points.

<i>Question</i>	<i>Answer</i>
<i>At what radio frequency does an AP communicate?</i>	In the U.S., wireless LAN radios transmit and receive on one of 11 channels in the 2.4-GHz frequency band. This is a public band, and does not require a license from the FCC.
<i>How do I secure the data crossing an AP's radio link?</i>	Enable the Wired Equivalent Privacy (WEP) function to encrypt the payload of packets sent across a radio link.
<i>What are possible sources of interference for the radio frequency link of the AP?</i>	Interference can come from a number of sources, including 2.4-GHz cordless phones, improperly shielded microwave ovens, and wireless equipment manufactured by other companies. Police radar, electric motors, and moving metal parts of machinery can cause interference too.
<i>How do I set the Outdoor AP back to its factory default settings?</i>	You can apply <i>Factory Reset</i> option from the menu of the WLAN Management System (WMS) or use <i>Kick Start</i> function by the following way: <ol style="list-style-type: none">1. Connect the Outdoor AP to your PC. Please make sure the Ethernet connection is normal.2. Open WLAN Management System (WMS) application and click Kick Start icon.3. Click <i>Find</i> icon from WLAN Kick Start window or press <F5> key to search the Outdoor AP.4. Right-click the Outdoor AP that you want to reset and select <i>Restore Default</i> option.

Troubleshooting

This section provides you with some troubleshooting info should you encounter installation or operation problems on Outdoor Access Point. If the problems still cannot be remedied after going through the Troubleshooting section, check the FAQs on page 45 of this manual.

If your problems still cannot be remedied after going through the FAQs and this Troubleshooting section, contact your network equipment supplier for assistance (see “Technical Support,”).

<i>Symptom</i>	<i>Suggested Solutions</i>
<i>The WMS utility cannot detect an Outdoor AP on the same network.</i>	<ol style="list-style-type: none">1. Make sure the Outdoor AP is powered on and connected to an Ethernet network.2. Check the IP addresses assigned to the Outdoor AP and WMS terminal PC. They should be in the same subnet and unique. For example, if the Outdoor AP's IP address is 192.168.1.5 with a mask of 255.255.255.0, then the PC's IP address should be 192.168.1.x with a mask of 255.255.255.0.
<i>Transmission performance is slow or erratic.</i>	<ol style="list-style-type: none">1. Change the direction of the antenna slightly.2. There may be interference, possibly caused by a microwave oven, 2.4-GHz wireless phone, or metal objects. Move these interference sources or change the location of the wireless PC or AP.3. Change the wireless channel on the Outdoor AP.4. Check that the Outdoor AP's antenna, connectors, and cabling are firmly connected.

Technical Support

If assistance is required, call your supplier for help. Have the following information ready before you make the call.

1. LED status
2. A list of the product hardware (including revision levels), and a brief description of the network structure
3. Details of recent configuration changes, if applicable

If it appears that more in-depth support is required, have the following information on hand before seeking assistance:

- What you were doing when the error occurred
- What error messages you saw
- Whether the problem can be reproduced
- The serial number of the product
- The firmware version and the debug information

From time to time updated firmware may be released. Contact your network equipment supplier for details

Limited Warranty

Hardware

The manufacturer warrants its products to be free of defects in workmanship and materials, under normal use and service, for a period of 12 months from the date of purchase from the manufacturer or its Authorized Reseller, and for the period of time specified in the documentation supplied with each product.

Should a product fail to be in good working order during the applicable warranty period, the manufacturer will, at its option and expense, repair or replace it, or deliver to the purchaser an equivalent product or part at no additional charge except as set forth below. Repair parts and replacement products are furnished on an exchange basis and will be either reconditioned or new. All replaced products and parts will become the property of the manufacturer. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

The manufacturer shall not be liable under this warranty if its testing and examination disclose that the alleged defect in the product does not exist or was caused by the purchaser's, or any third party's misuse, neglect, improper installation or testing, unauthorized attempt to repair or modify, or any other cause beyond the range of the intended use, or by accident, fire, lightning, or other hazard.

Software

Software and documentation materials are supplied "as is" without warranty as to their performance, merchantability, or fitness for any particular purpose. However, the media containing the software is covered by a 90-day warranty that protects the purchaser against failure within that period.

Limited Warranty Service Procedures

Any product (1) received in error, (2) in a defective or non-functioning condition, or (3) exhibiting a defect under normal working conditions, can be returned to the manufacturer by following these steps:

You must prepare:

- Dated proof of purchase
 - Product model number and quantity
 - Product serial number
 - Precise reason for return
 - Your name/address/email address/telephone/fax
1. Inform the distributor or retailer.
 2. Ship the product back to the distributor/retailer with prepaid freight. The purchaser must pay the shipping fee from the distributor/retailer to manufacturer. Any package sent C.O.D. (Cash On Delivery) will be refused.
 3. Charges: Usually RMA (Returned Material Authorization) items will be returned to the purchaser via airmail, prepaid by the manufacturer. If returned by another carrier, the purchaser will pay the difference. A return freight and handling fee will be charged to the purchaser if the manufacturer determines that the product was not faulty or that the damage was caused by the user.

Warning

The manufacturer is not responsible for the integrity of any data on storage equipment (hard drives, tape drives, floppy diskettes, etc.). We strongly recommend that our customers back their data up before sending such equipment in for diagnosis or repair.

Service after Warranty Period

After the warranty period expires, all products can be repaired for a reasonable service charge. The shipping charges to and from the manufacturer's facility will be borne by the purchaser.

Return for Credit

In the case of a DOA (Dead on Arrival) or a shipping error, a return for credit will automatically be applied to the purchaser's account, unless otherwise requested.

Limitation of Liability

All expressed and implied warranties of a product's merchantability, or of its fitness for a particular purpose, are limited in duration to the applicable period as set forth in this limited warranty, and no warranty will be considered valid after its expiration date.

If this product does not function as warranted, your sole remedy shall be repair or replacement as provided for above. In no case shall the manufacturer be liable for any incidental, consequential, special, or indirect damages resulting from loss of data, loss of profits, or loss of use, even if the manufacturer or its authorized distributor/dealer has been advised of the possibility of such damages, or for any claim by any other party.

Regulatory Domains and Channels

This appendix lists the channels supported by the world’s regulatory domains.

The channel numbers, channel center frequencies, and regulatory domains are shown in the table.

<i>Channel Number</i>	<i>Center Frequency (MHz)</i>	<i>FCC/Canada</i>	<i>ETSI</i>	<i>Spain</i>	<i>France</i>	<i>Japan</i>
1	2412	O	O			O
2	2417	O	O			O
3	2422	O	O			O
4	2427	O	O			O
5	2432	O	O			O
6	2437	O	O			O
7	2442	O	O			O
8	2447	O	O			O
9	2452	O	O			O
10	2457	O	O	O	O	O
11	2462	O	O	O	O	O
12	2467		O		O	O
13	2472		O		O	O
14	2484					O